SCHIFF HARDIN & WAITE
A Partnership Including Professional Corporations

6600 Sears Tower, Chicago, Illinois 60606-6360
Telephone (312) 258-5500 Facsimile (312) 258-5600

Chicago
Washington
New York
Dublin
Atlanta

Mark Bergner
(312) 258-5779
Email: mbergner@schiffhardin.com

Patent Department Facsimile: (312) 258-5921

December 1, 2003

U.S. EXPRESS MAIL
#EL843735598US

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

RE: Patent Application for Karlheinz Dorn et al Entitled "PROCEDURE FOR USER LOGIN TO DATA PROCESSING DEVICES" Claiming Priority From German 102 56 078.1 of November 29, 2002 and U.S. Provisional Application Serial No. 60/430,206 of December 2, 2002, Our Case No. P02,0630-01.

S I R:

Under the provisions of 37 CFR 1.41(c), I am filing on behalf of the inventors, Karlheinz Dorn, Ivan Murphy, Thomas Pohley and Andreas Schuelke, the attached patent application with one set of drawings containing 4 sheets with 5 Figures, an unsigned Declaration, a Certified Copy of German 102 56 078.1 of 29 November 2002 and a Certified Copy of Provisional Application 60/430,206 of December 2, 2002 (from which priority is claimed) and appropriate government filing fee.

On behalf of the inventors, I hereby claim priority from German Application No. 102 56 078.1 of 29 November 2002 and U.S. Provisional Application No. 60/430,206 of December 2, 2002.

I request that the application be assigned a Serial No. and Filing Date pursuant to the provisions of 37 CFR 1.53(b) and 37 CFR 1.53(f).

Very sincerely,

Mark Bergner

Mark Bergner
(Reg. No. 45,877)
SCHIFF HARDIN & WAITE

MB/pav

Enclosures

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	102 56 078.1
Anmeldetag:	29. November 2002
Anmelder/Inhaber:	Siemens Aktiengesellschaft, München/DE
Bezeichnung:	Verfahren zum Anmelden von Nutzern an Datenverarbeitungseinrichtungen
IPC:	G 06 F 12/14

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 4. November 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Kahle

A 9161
06/00
EDV-L

Beschreibung

Verfahren zum Anmelden von Nutzern an Datenverarbeitungseinrichtungen

Die Erfindung betrifft ein Verfahren zum schnellen Anmelden von Nutzern an Datenverarbeitungseinrichtungen.

Die Verarbeitung elektronischer Daten durch Datenverarbeitungseinrichtungen in Arbeitsumgebungen mit sensiblen Daten erfordert einen wirksamen Schutz der Daten vor unberechtigten Zugriffen. Es muss jederzeit sichergestellt sein, dass eine Einsichtnahme oder Veränderungen z.B. von elektronischen Patientenakten oder Bildern aus digitalen diagnostischen Bildgebungsverfahren ausschließlich durch berechtigte Personen erfolgen kann. Darüber hinaus müssen in medizinischen Arbeitsumgebungen sämtliche Zugriffe auf die sensiblen Daten so protokolliert werden, dass jederzeit nachvollziehbar ist, welche Personen Datenzugriffe welcher Art vorgenommen haben.

Bei herkömmlichen Datenträgern, wie etwa Patientenakten auf Papier oder diagnostischen Bildern auf Filmsystemen, ist eine Kontrolle des Datenzugriffs durch Kontrolle des Verbleibs der Datenträger ohne weiteres möglich. Dahingegen sind elektronische Daten ohne weiteres vielfach zugreifbar und statt des Verbleibs der Daten müssen Zugriffe darauf kontrolliert werden. Zu diesem Zweck müssen sich Nutzer von Datenverarbeitungseinrichtungen für sensible Daten, wie medizinischen Computer-Arbeitsplätzen, durch Eingabe von Nutzernamen und Passwörtern oder durch biometrische Identifikation, z.B. anhand des Fingerabdrucks, oder durch Chipkarten o.ä. identifizieren, um durch die Datenverarbeitungseinrichtung authentifiziert werden zu können. Im Rahmen der Authentifizierung wird die Identität des jeweiligen Nutzers zu Protokollierungszwecken festgestellt und der Daten- und Anwendungszugriff im für den jeweiligen Nutzer vorgesehenen Umfang autorisiert. Außer-

dem wird der Umfang der Zugriffsmöglichkeiten auf Hardware und Software festgelegt.

Im klinischen Alltag arbeiten oft mehrere Personen, z.B. medizinisch-technische Assistentinnen oder Ärzte, abwechselnd an der gleichen Datenverarbeitungseinrichtung, z.B. einem Computer-Arbeitsplatz zur Befundung oder zur Erstellung diagnostischer Bilder. Um dem Anspruch rationeller und ökonomischer Arbeitsabläufe gerecht zu werden, muss der Nutzerwechsel möglichst schnell durchführbar sein. Soll mit der gleichen Datenverarbeitungseinrichtung oder den gleichen Patientendaten weitergearbeitet werden, müssen auch diese nach einem Nutzerwechsel möglichst schnell wieder verfügbar sein.

Bislang erfolgt die Authentifizierung eines Nutzers durch die Datenverarbeitungseinrichtung auf Betriebssystem-Ebene. Das sogenannte Login am Betriebssystem wird beim Systemstart durch Eingabe eines Nutzernamens und eines Passworts identifiziert, und in Abhängigkeit von der Identifikation werden durch das Betriebssystem Zugriffsrechte für Daten, Hardware und Software zuerkannt. Diese Authentifizierung auf Ebene des Betriebssystems, z.B. Windows, weist den schwerwiegenden Nachteil auf, dass zum Nutzerwechsel der Zugriff auf sämtliche Patientendaten beendet werden, alle Anwendungen gestoppt und das Betriebssystem heruntergefahren und wieder hochgefahren werden muss. Diese Abläufe sind äußerst zeitaufwändig. Darüber hinaus steht dem nächsten Nutzer nicht der aktuelle Stand der Benutzeroberfläche und der darin enthaltenen Patientendaten zur Verfügung, falls diese als temporäre Informationen beim Herunterfahren des Betriebssystems verloren gehen.

Als Abhilfe wird bei der Authentifizierung auf Betriebssystem-Ebene daher bislang mit sogenannten Gruppen-Accounts gearbeitet, die durch Gruppen von Nutzern verwendet werden, die sämtlich die gleichen Zugriffsrechte erhalten sollen. Die Authentifizierung von Nutzern im Rahmen von Gruppen-Accounts

bringt jedoch den Nachteil mit sich, dass weder durch die Datenverarbeitungseinrichtung noch durch die darauf laufenden Anwendungs-Programme feststellbar ist, welcher Nutzer jeweils aktuell arbeitet. Da dies die Protokollierung der Datennutzeraktionen unmöglich machen würde, erfolgen Nutzerwechsel bei Benutzung von Gruppen-Accounts dadurch, dass die laufende Anwendung beendet und durch den neuen Nutzer neu gestartet werden muss. Temporäre Daten der laufenden Anwendung gehen zwar auch beim Beenden der Anwendung statt des Betriebssystems verloren, der Zeitverlust ist jedoch gegenüber dem Neustart des Betriebssystems geringer.

Der unter Aspekten ökonomischer Arbeitsweise nicht vertretbare Zeitverlust führt bislang häufig dazu, dass Nutzer an bildgebenden medizinischen Datenverarbeitungseinrichtungen nicht authentifiziert werden. Stattdessen erfolgen Identifikation und Autorisierung von Nutzern durch die rein physische Kontrolle des Zugriffs auf die bildgebende Einrichtung, d.h. durch eine simple Zugangskontrolle zu dem Raum in dem die Einrichtung steht. Insbesondere die Protokollierung von Datenzugriffen durch Nutzer ist an einer solchen Einrichtung nur indirekt möglich, in dem z.B. abgeglichen wird, welcher Nutzer zum Zeitpunkt eines Datenzugriffs in dem Raum der Einrichtung zugegen war. Diese Art der Protokollierung ist aufwändig und langfristig nicht im Nachhinein rekonstruierbar.

Die beschriebenen Nachteile treten vor allem in medizinischen Arbeitsumgebungen auf, wo bereits grundsätzlich unter großem Zeitdruck gearbeitet wird, der sich in Notfallsituationen noch wesentlich verschärfen kann. Sie wirken sich jedoch auch auf andere Datenverarbeitungseinrichtungen aus, die mit sensiblen Daten arbeiten, z.B. im Finanzwesen, in Forschung und Entwicklung, im Versicherungswesen oder bei der Bearbeitung demografischer Fragen.

Die Aufgabe der Erfindung besteht darin, ein Verfahren zum schnellen Anmelden von Nutzern an Datenverarbeitungseinrich-

tungen anzugeben, an denen sensible Daten verarbeitet werden und an denen daher die Authentifizierung des Nutzers erforderlich ist. Unter sensiblen Daten sollen dabei insbesondere personenbezogene Angaben zum gesundheitlichen oder finanziellen Status oder in sonstigem Bezug zu Persönlichkeitsrechten verstanden werden.

Die Erfindung löst diese Aufgabe durch ein Verfahren mit den Verfahrensschritten des ersten Patentanspruchs.

Ein Grundgedanke der Erfindung besteht darin, die Anmeldung von Nutzern an Datenverarbeitungseinrichtungen durch eine Authentifizierungs-Instanz erfolgen zu lassen, die unabhängig vom Login an einem Betriebssystem oder einer laufenden Anwendung arbeitet. Unabhängig soll dabei so verstanden werden, dass die Anmeldung eines Nutzers nicht den Neustart des Betriebssystems oder der Anwendung erforderlich macht. Unter Authentifizierung sollen dabei die Identifikation einer Person und die Zuerkennung von Zugriffsrechten für Daten, Software und Hardware für diese Person verstanden werden. Die Authentifizierungs-Instanz ermöglicht den Wechsel des Nutzers, also eine Neu-Authentifizierung, bei laufendem Betriebssystem und laufender Anwendung oder Anwendungen.

Dadurch kann ein Nutzerwechsel zum einen schnell durchgeführt werden, da der Zeitaufwand für das Beenden und Neustarten von Anwendung oder Betriebssystem eingespart wird. Zum anderen kann ein neuer Nutzer nach Nutzerwechsel sämtlichen temporären Daten, wie aktuell bearbeitete Patientendaten oder die aktuelle Konstellation der Anwendung oder Anwendungen weiter benutzen, da sie nicht durch einen Neustart verloren gehen. Weiter ist der Nutzerwechsel ausreichend schnell, um insbesondere an Datenverarbeitungseinrichtungen eingesetzt werden zu können, an denen unter enormem Zeitdruck gearbeitet werden muss. Dadurch kann auch an solchen Einrichtungen eine ständig aktuelle Nutzer-Identität ermittelt werden, die z.B. zur

vollständigen Protokollierung aller Zugriffe genutzt werden kann.

In einer vorteilhaften Ausgestaltung der Erfindung ermöglicht die Authentifizierungs-Instanz den Nutzerwechsel unter Beibehaltung aller temporären Daten, wie aktuell bearbeiteten Patientendaten, aktuellen Anwendungseinstellungen oder Sichten, in Abhängigkeit von einer Eingabe eines Nutzers, der dies wünscht. Es wird also Daten und der gesamte Anwendungs-Kontext erhalten. Durch die Beibehaltung des aktuellen Status können verschiedene Nutzer an der gleichen Datenverarbeitungseinrichtung die gleichen Daten in gleichbleibendem Anwendungs-Kontext in schnellem Wechsel bearbeiten. Gleichzeitig ist durch die Neu-Authentifizierung bei Nutzerwechsel jederzeit gewährleistet, dass die abwechselnden Nutzer jeweils ausreichende Zugriffsrechte besitzen, um mit den gleichen Daten arbeiten zu dürfen.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung werden sämtliche Nutzeraktionen unter Angabe von Informationen zu deren Identität protokolliert. Die für die Protokollierung zu verwendende Identität wird dabei durch die Authentifizierungs-Instanz vorgegeben, die jeweils Identität und Autorisierung gleichzeitig ermittelt. Dadurch kann gewährleistet werden, dass sämtliche Datenzugriffe unter Angabe aktueller Nutzer-Identitäten der Protokollierung zugeführt werden, da durch die Authentifizierungs-Instanz Datenzugriffe ohne Vorliegen einer Nutzer-Identität nicht autorisiert werden.

In einer weiteren vorteilhaften Ausgestaltung ermöglicht die Authentifizierungs-Instanz den Nutzerwechsel mit gleichzeitiger Löschung des aktuellen Status der bearbeiteten Daten und der Benutzeroberfläche, d.h. der aktuellen Bildschirm-Ansichten. Die Löschung erstreckt sich dabei ausschließlich auf temporäre Daten während dauerhaft gespeicherte Daten erhalten bleiben. Der Nutzerwechsel mit Löschung des aktuellen

Status erfolgt auf eine entsprechende Eingabe des aktuellen Nutzers hin. Er ermöglicht es dem Nutzer, sich von der Bearbeitung von Daten sowie von der laufenden Anwendung abzumelden, ohne dass dafür die Anwendung oder gar das Betriebssystem beendet werden müssten.

Dadurch kann ein Nutzer seine Arbeit an der Datenverarbeitungseinrichtung beenden ohne dass der nachfolgende Nutzer die Anwendung oder gar das Betriebssystem neu starten müsste. Dies erspart dem nachfolgenden Nutzer den mit einem Neustart verbundenen Zeitaufwand, da er nach seiner Authentifizierung an der Einrichtung unmittelbar in der laufenden Anwendung weiterarbeiten kann.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung wird der Nutzerwechsel bei Eintreten einer bestimmten Bedingung, z.B. nach Zeitablauf, analog zu einem Bildschirmschoner automatisch initiiert. Dabei werden ebenso wie bei einem Bildschirmschoner die aktuell dargestellten Anwendungsdaten temporär gelöscht, also unkenntlich gemacht aber in der Einrichtung beibehalten. Durch Ausführen einer Aktion an der Datenverarbeitungseinrichtung bei aktivierter Bildschirmschoner-Instanz, z.B. Tastendruck oder Mausbewegung, wird eine Abfrage zur aktuellen Authentifizierung des Nutzers ausgelöst. Wird durch die Authentifizierung festgestellt, dass der Nutzer nicht gewechselt hat, wird der vorige Status der Darstellung und der temporären Datenstände wieder hergestellt und die Arbeit kann fortgesetzt werden. Wird in Abweichung davon festgestellt, dass ein anderer Nutzer mit geringeren Zugriffsrechten an der Einrichtung arbeiten will, wird der vorherige Darstellungsstatus und temporäre Datenstand gelöscht oder in seinem Inhalt um die nicht zugriffsberechtigten Teile reduziert. Temporären Anwendungsdaten gehen bei der Reduzierung verloren. Wird statt dessen festgestellt, dass der neue Nutzer weitergehende Zugriffsrechte besitzt, so kann je nach vorgebbaren Einstellungen entweder der vorherige An-

zeigestatus und Datenstand wieder hergestellt oder ebenfalls inhaltlich reduziert werden.

Die Funktionalität in Anlehnung an einen Bildschirmschoner erhöht die Sicherheit der Einrichtung im Umgang mit sensiblen Daten, da die Einrichtung z.B. in Fällen, in denen der Nutzer die Arbeit plötzlich und ohne vorherige Abmeldung beenden muss, Zugriffe automatisch sperrt und eine Neu-Authentifizierung verlangt.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung veranlasst die Authentifizierungs-Instanz bei fehlerhaften Eingaben zur Identität oder Passwort eines Nutzers automatisch eine Sperrung der Einrichtung auf Betriebssystem-Ebene, z.B. durch Herunterfahren des Betriebssystems. Dadurch wird die Sicherheit im Umgang mit den durch die Einrichtung verarbeiteten sensiblen Daten erhöht, da Fehleingaben durch nicht berechtigte Personen automatisch zu einem Zustand der Einrichtung führen, das maximalen Zugriffsschutz bietet. Insbesondere werden so Möglichkeiten zur Manipulation der Authentifizierungs-Instanz durch Schwachstellen, die vom Betriebssystem aus angreifbar wären, ausgeschlossen. Die Sperrung von Datenzugriffen auf Ebene des Betriebssystems bildet die höchste Barriere gegenüber Manipulationsversuchen.

Nachfolgend werden Ausführungsbeispiele der Erfindung anhand von Figuren näher erläutert. Es zeigen:

FIG 1 Systemarchitektur mit Authentifizierungs-Instanz,
FIG 2 Authentifizierungs-Verfahren als Flussdiagramm.

In **FIG 1** ist eine Systemarchitektur zur Ausführung des erfundenen Verfahrens schematisch dargestellt. Die Darstellung gibt lediglich die funktionalen Instanzen der Architektur wieder, ohne direkten Bezug auf einrichtungsmäßige Repräsentationen dieser Instanzen, z.B. durch bestimmte Hardware-Komponenten, zu nehmen.

Dargestellt ist ein erstes Anwendungs-Programm 71 und ein zweites Anwendungs-Programm 73 zur Verarbeitung sensibler Daten. Bei den sensiblen Daten kann es sich z.B. um medizinische Befunddaten, diagnostische Bilddaten, Informationen zu Finanzen oder zu Versicherungen oder demographische Daten handeln. Die Daten sollen dadurch als sensibel charakterisiert sein, dass sie, wenigstens teilweise, geheimhaltungsbedürftig sind und nur berechtigten Nutzern zugänglich sein sollen.

Die Anwendungs-Programme 71,73 können z.B. Bildgebungsprogramme in der medizinischen Diagnostik, Betrachtungsprogramme für elektronische Patientendaten, Programme für finanzielle Transaktionen, statistische Auswertungen oder Buchhaltung sein. Durch die Anwendungs-Programme 71,73 kann ein Nutzer Daten einsehen, verändern, erzeugen oder löschen. Im Rahmen der Bearbeitung von Daten können außerdem andere Anwendungs-Programme gestartet oder die Anwendungs-Programme 71,73 beendet werden. Es spielt dabei keine Rolle, ob nur ein oder mehrere Anwendungs-Programme 71, 73 gestartet werden. Wesentlich ist lediglich, dass sie über eine gemeinsame Schnittstelle, wie sie in ähnlicher Weise von Bildschirmschoner-Schnittstellen bekannt ist, mit der unten beschriebenen Authentifizierungs-Instanz 75 kommunizieren können.

Die Anwendungs-Programme 71,73 sind durch eine Authentifizierungs-Instanz 75 abgesichert, die sämtliche Zugriffe kontrolliert. Die Authentifizierungs-Instanz 75 stellt die Identität des Nutzers fest, indem entweder die Eingabe eines Nutzernamens und eines Passworts gefordert wird, oder indem auf eine biometrische Messeinrichtung, z.B. zur Ermittlung des Fingerabdrucks oder der Irisgestalt oder auf einen Chip oder Tranponder, Lesgerät zugegriffen wird.

In Abhängigkeit von der ermittelten Identität ordnet die Authentifizierungsinstanz 75 dem Nutzer Zugriffsrechte für Da-

ten, Software und Hardware zu. Sie kann dabei über alle Zugriffsrechte, die das Betriebssystem 79 ihr gewährt, verfügen; das Betriebssystem 79 gibt als den maximal möglichen Umfang an Zugriffsrechten vor. Dies schließt den Zugriff auf Daten 87, Hardware 85 und Software 71,73 ein, so dass die Authentifizierungs-Instanz 75 die Benutzung aller Einrichtungs-Resourcen einschließlich der Anwendungs-Programme 71,73 freigeben oder Sperren kann.

Insofern arbeitet die Authentifizierungs-Instanz 75 zwar in dem vom Betriebssystem 79 vorgegebenen Rahmen und nur dann, wenn auch das Betriebssystem 79 gestartet wurde. Innerhalb des vorgegebenen Rahmens arbeitet sie jedoch unabhängig vom Betriebssystem 79 und insbesondere unabhängig von einem Neu-Start des Betriebssystems 79. Zugriffe durch den Nutzer erfolgen ausschließlich über die Benutzeroberfläche 81, die durch die Authentifizierungs-Instanz 75 kontrolliert wird.

Die Authentifizierungs-Instanz 75 weist zwei Unterinstanzen auf, eine Bildschirmschoner-Instanz 76 und eine Instanz zum Nutzerwechsel 77. Die Bildschirmschoner-Instanz 76 sorgt ähnlich bekannten Bildschirmschonern dafür, dass die Benutzeroberfläche 81 bei Eintreten bestimmter Bedingungen, z.B. nach Zeitablauf, gelöscht wird. Mit gelöscht ist gemeint, dass die bildliche Darstellung der Benutzeroberfläche 81 auf einem Anzeigegerät, z.B. einem Bildschirm, so verändert wird, dass keine geheimhaltungsbedürftigen Daten mehr angezeigt werden, sie wird also inhaltlich reduziert bzw. neutralisiert. Damit soll verhindert werden, dass nach eiligem Verlassen der Einrichtung ohne ordnungsgemäße Abmeldung durch den vorhergehenden Nutzer sensible Daten unkontrolliert einsehbar bleiben.

Die Bildschirmschoner-Instanz 76 kann in Analogie zu bekannten Bildschirmschonern dadurch aktiviert werden, dass eine bestimmte Zeit ohne jedwede Nutzereingabe an der Einrichtung verstrichen ist. Zur Erhöhung der Datensicherheit kann jedoch

auch vorgesehen sein, dass die Bildschirmschoner-Instanz 76 unabhängig von Nutzereingaben aktiviert wird.

Um die Bildschirmschoner-Instanz 76 zu deaktivieren und zur ursprünglichen Benutzeroberfläche 81 zurückzugelangen, muss sich der Nutzer erneut, wie oben beschrieben, identifizieren lassen. Die Darstellung der Benutzeroberfläche 81 nach der Deaktivierung hängt davon ab, ob der Nutzer inzwischen gewechselt hat und ggf. welchen Umfang die Rechte eines neuen Nutzers aufweisen. Sie kann je nachdem inhaltlich unverändert bleiben oder inhaltlich verändert sein.

Fand kein Nutzerwechsel statt und wurde lediglich der vorherige Nutzer erneut authentifiziert, so steht nach Deaktivierung der Bildschirmschoner-Instanz 76 die Benutzeroberfläche 81 in exakt dem Zustand wieder zur Verfügung, den sie vor Aktivierung der Bildschirmschoner-Instanz 76 hatte, der gesamte Anwendungs-Kontext bleibt also erhalten. Dies schließt den Status der laufenden Anwendungen, z.B. welche Fenster geöffnet sind und welche Anwendungs-Module geladen sind, ebenso wie die aktuell angezeigten sensiblen Daten ein und deren temporären Bearbeitungsstatus. Auch temporäre Änderungen der Daten, die noch nicht durch die Datenverarbeitungseinrichtung gespeichert wurde, stehen wie vorher zur Verfügung und können gespeichert oder zur weiteren Verarbeitung genutzt werden.

Hat jedoch ein Nutzerwechsel stattgefunden und stellt sich durch die Authentifizierung heraus, dass der neue Nutzer gegenüber dem vorhergehenden Nutzer eingeschränkte Zugriffsrechte hat, so wird die Benutzeroberfläche 81 je nach Umfang und Art der Einschränkung inhaltlich reduziert oder völlig neutral gemacht, der Anwendungs-Kontext bleibt also nur eingeschränkt erhalten. Hat der neue Nutzer z.B. keine Berechtigung, auf die zuvor angezeigten Daten zuzugreifen, so werden diese aus der Benutzeroberfläche 81 entfernt und sind auch durch die Anwendungs-Programme 71,73 nicht mehr zugänglich. Hat der neue Nutzer z.B. nur Berechtigung zur Einsichtnahme

und nicht zur Veränderung von Daten, so werden evt. gesperrte Datenveränderungsmodule der Anwendungs-Programme 71,73 aus der Benutzeroberfläche 81 entfernt, oder reine Datenverarbeitungsanwendungen geschlossen.

Hat der neue Nutzer gegenüber dem vorhergehenden erweiterte Rechte, so kann je nach vorgebbarer Einstellung entweder der vorherige Anwendungs-Kontext, also Benutzeroberfläche 81 samt aktuellen Daten, vollständig wieder hergestellt werden oder ein beliebiger anderer Zustand, z.B. ein erweiterter Umfang an sensiblen Daten oder Funktionsmodulen der Anwendungs-Programme 71,73 verfügbar gemacht werden.

Die Nutzerwechsel-Instanz 77 wird zum einen in Abhängigkeit von der Aktivierung der Bildschirmschoner-Instanz 76 aktiv, zu dessen Deaktivierung eine erneute Authentifizierung des Nutzers erforderlich ist. Zum anderen kann die Nutzerwechsel-Instanz 76 auch durch den Nutzer aktiviert werden. Die Aktivierung erfolgt z.B. dann, wenn der Nutzer sich von der Einrichtung durch eine entsprechende Eingabe abmeldet. Auf die Abmeldung hin werden sämtliche aktuell angezeigten Daten aus der Benutzeroberfläche 81 und aus den Anwendungs-Programmen 71,73 entfernt, wobei sämtliche temporären Informationen wie vorläufige Änderungen der Daten oder der aktuelle Status der Anwendungs-Programme 71,73 ab sofort nicht mehr zur Verfügung stehen. Je nach vorgebbarer Einstellung können temporäre Daten entweder vollständig verworfen oder automatisch gespeichert werden. Die laufende Anwendungs-Programme 71,73 wird dadurch in einen neutralen Ausgangszustand zurückversetzt, in dem der folgende Nutzer seine Arbeit beginnen kann.

Durch eine entsprechende Eingabe des Nutzers kann die Nutzerwechselinstanz 77 jedoch auch veranlassen, dass der aktuelle Nutzer abgemeldet wird, jedoch sämtliche temporären Daten weiterhin auf der Benutzeroberfläche 81 zur Verfügung stehen. Diese Möglichkeit ist vor allem dann von Bedeutung, wenn der folgende Nutzer mit den aktuell angezeigten Daten im gegen-

wärtigen Status der Anwendungs-Programme 71,73 weiterarbeiten soll. Durch einen derartigen Wechsel des Nutzers bleibt die Autorisierung von Zugriffsrechten erhalten, während die Identität des Nutzers wechselt. Die jeweils aktuelle Nutzer-Identität steht dann zur vollständigen Protokollierung aller laufenden Nutzeraktionen und Zugriffe zur Verfügung.

Stellt die Nutzerwechsel-Instanz 77 bei der Neu-Authentifizierung des Nutzers fest, dass dieser geringere Rechte besitzt als der vorhergehende Nutzer, so dass temporäre Daten auf der Benutzeroberfläche 81 nicht mehr dargestellt werden dürften und verloren gehen würden, so kann an den Nutzer eine entsprechende Warnmeldung ausgegeben werden, z.B. in einem entsprechenden Hinweis-Fenster auf der Benutzeroberfläche 81. Dadurch besteht für den vorhergehenden Nutzer die Möglichkeit, durch eigene Anmeldung an der Einrichtung den vorherigen, temporären Status der Daten und Programm-Sichten wieder herzustellen und nötigenfalls in der Einrichtung zu speichern. Falls dies nicht gewünscht wird, so kann durch Bestätigung der Warnmeldung ein neuer Anwendungs-Status mit veränderter Benutzeroberfläche 81 und unter Inkaufnahme von Verlusten temporärer Daten erzeugt werden.

An der in FIG 1 gewählten zeichnerischen Darstellung wird sichtbar, dass die Authentifizierungs-Instanz 75 samt Benutzeroberfläche 81 auf die Anwendungs-Programme 71,73 sowie das laufende Betriebssystem 79 aufsetzt. Dies ist für die Erfindung von großer Bedeutung, da die Zugriffskontrolle auf einer Ebene stattfindet, die oberhalb der Betriebssystem-Ebene 79 und der Anwendungs-Programm-Ebene 71,73 angesiedelt ist. Daher können Änderungen der Nutzer-Autorisierung und -Identifizierung vorgenommen werden, ohne dazu laufende Anwendungs-Programme 71,73 oder dass Betriebssystem 79 neu starten zu müssen. Dies beschleunigt die Neu-Authentifizierung bei Nutzerwechsel erheblich.

Die Möglichkeit zum schnellen Nutzerwechsel macht das Verfahren an Arbeitsplätzen praktikabel, an denen unter großem Zeitdruck gearbeitet werden muss, z.B. in der Medizin oder Notfall-Medizin. Infolge dessen steht an solchen Arbeitsplätzen durch Verwendung des Verfahrens die Möglichkeit des laufenden, vollständigen Protokollierung aller Nutzeraktionen zur Verfügung. Eine derartige Protokollierung ist insbesondere durch den Datenschutz im Gesundheitswesen zwingend vorgeschrieben. Ein weiterer Vorteil besteht darin, dass Arbeitsplätze, die durch einen Bildschirmschoner geschützt werden, nicht mehr dadurch blockiert werden können, dass das Bildschirmschoner-Passwort des vorherigen Nutzers oder das generelle Bildschirmschoner-Passwort nicht bekannt ist. Statt dessen erfolgt die Deaktivierung der Bildschirmschoner-Instanz 76 durch eine Neu-Authentifizierung des Nutzers, der dadurch seine eigenen Identifikations-Daten eingeben muss.

In **FIG 2** sind die Schritte des Verfahrens als Flussdiagramm dargestellt. In Schritt 1 erfolgt die Anmeldung am Betriebssystem, das in Schritt 3 in einer von der Anmeldung abhängigen Betriebssystem-Konfiguration arbeitet. Die Zugriffsrechte bei Anmeldungen am Betriebssystem sind so beschaffen, dass die Kontrolle aller Zugriffe durch die Authentifizierungs-Instanz 75 gewährleistet werden kann. Eine Anmeldung am Betriebssystem 79 mit umfassenden Datenzugriffsrechten bleibt dabei Systemadministratoren vorbehalten, während Anwendungsnutzer nur Zugriff über die Authentifizierungs-Instanz 75 erhalten.

In Schritt 5 wird das Anwendungs-Programm 71,73 gestartet. Da bereits die Nutzung des Anwendungs-Programms 71,73 der Einschränkung von Zugriffsrechten unterliegen kann, wird unmittelbar nach dem Starten des Anwendungs-Programms 71,73 oder der Anwendungs-Programme 71,73 in Schritt 7 die Eingabe eines Nutzer-Logins gefordert. Die Eingabe kann, wie oben beschrieben, durch manuelle Eingabe von Daten oder Messungen biometrischer oder sonstiger Informationen erfolgen. Sie kann zum

Beispiel über ein Login-Fenster ähnlich dem bei der Betriebssystem-Anmeldung auf der Benutzeroberfläche 81 erfolgen oder durch ein Hinweis-Fenster auf der Benutzeroberfläche 81 vom Nutzer angefordert werden.

Kann bereits das Nutzer-Login nicht identifiziert werden, so wird die Datenverarbeitungseinrichtung im folgenden Schritt 11 für weitere Eingaben gesperrt. Andernfalls wird in Schritt 9 ein Nutzer-Passwort erfragt, wobei bei Verwendung von biometrischen Daten oder Chipkarten die Schritte 7 und 9 zusammenfallen. Kann das Nutzer-Passwort in Schritt 9 nicht verifiziert werden, erfolgt ebenfalls im Schritt 11 die Sperrung sämtlicher Zugriffe. Die Sperrung der Zugriffe in Schritt 11 kann derart erfolgen, dass weitere Zugriffsmöglichkeiten nur für Systemadministratoren bestehen oder dass das System heruntergefahren wird, um sämtliche Manipulationen zu verhindern. Die Sperrung kann jedoch auch lediglich darin bestehen, dass die Login- und Passwort-Prozedur erneut gestartet wird.

Können Login und Passwort erfolgreich verifiziert werden, wird die Identität des Nutzers festgelegt und in Schritt 13 erfolgt die Festlegung von Zugriffsrechten in der Einrichtung. Dies schließt die Rechte zur Verwendung von Anwendungs-Programmen 71,73 sowie Hardware 83 und den Zugriff auf sensible Daten 85 ein.

Im folgenden Schritt 15 werden die zugewiesenen Rechte daraufhin überprüft, ob ihr Umfang gegenüber den vor der Anmeldung des Nutzers herrschenden Rechten verändert ist.

Hat sich ein neuer Nutzer mit Rechten eines geringeren Umfangs als der vorherige Nutzer angemeldet, so werden in Schritt 17 die Datenzugriffsmöglichkeiten eingeschränkt und im folgenden Schritt 19 der verfügbare Umfang an Anwendungs-Programmen 71,73 bzw. Anwendungsmodulen ebenfalls reduziert.

Haben sich die Rechte in ihrem Umfang nicht verändert, z.B. weil sich derselbe Nutzer wie zuvor anmeldet oder weil sich ein neuer Nutzer derselben Autorisierungsklasse oder -Rolle anmeldet, so werden in Schritt 21 die Datenzugriffsrechte wieder hergestellt und in Schritt 23 der Funktionsumfang der Anwendungs-Programme 71,73, wodurch der vorherige Anwendungs-Kontext wieder hergestellt wird.

Hat sich der Umfang der Zugriffsrechte vergrößert, das z.B. der Fall sein kann, wenn zuvor kein Nutzer angemeldet war, so werden in Schritt 25 die Datenzugriffsrechte erweitert und in Schritt 27 ein erweiterter Funktionsumfang der Anwendungs-Programme 71,73 freigegeben.

Auf Basis der zugewiesenen Rechte wird in Schritt 29 die Benutzeroberfläche 81 aufgebaut und auf einem Sichtgerät, z.B. einem Computer-Bildschirm, dargestellt. Dabei werden nur Daten dargestellt, zu deren Einsichtnahme der angemeldete Nutzer berechtigt ist, und nur Funktionsmodule der Anwendungs-Programme 71,73 verfügbar gemacht, die der angemeldete Nutzer benutzen darf. Hat der Nutzer z.B. keine Berechtigung zur Veränderung von Daten, so werden Module der Anwendungs-Programme 71,73 zur Veränderung von Daten deaktiviert.

Im folgenden Schritt 31 arbeitet der Nutzer mit dem jeweiligen Anwendungs-Programm 71,73, wobei sämtliche Aktionen und Datenzugriffe in Schritt 33 unter Angabe der aktuell festgelegten Identität protokolliert werden, dass die nachträgliche Rekonstruktion sämtlicher Nutzeraktivitäten jederzeit möglich ist.

Im folgenden Schritt 35 hat der Nutzer die Möglichkeit, aktuelle Daten oder den aktuellen Status der Anwendungs-Programme 71,73 zu speichern.

Im folgenden Schritt 37 besteht die Möglichkeit, einen Nutzerwechsel zu initiieren. Schritt 37 kann z.B. durch eine

entsprechende Nutzer-Eingabe ausgelöst werden. Beim Nutzerwechsel wird der gegenwärtige Status der Benutzeroberfläche 81 beibehalten, sozusagen eingefroren, und die Neu-Authentifizierung eines neuen Nutzers im zuvor beschriebenen Schritt 7 gestartet. Es wird also ein Neu-Beginn des Verfahrens bei Schritt 7 mit der Möglichkeit, den Anwendungs-Kontext zu erhalten, ausgelöst.

Andernfalls besteht in Schritt 39 die Möglichkeit für den Nutzer, sich von dem Anwendungs-Programm 71,73 abzumelden. In diesem Fall wird im folgenden Schritt 41 die Benutzeroberfläche 81 gelöscht. Dabei werden sämtliche angezeigten Daten 85 entfernt und das Anwendungs-Programm 71,73 in einen neutralen Status versetzt. Anschließend kann sich ein neuer Benutzer im zuvor beschriebenen Schritt 7 anmelden.

Andernfalls besteht in Schritt 43 die Möglichkeit, das Anwendungs-Programm 71,73 zu beenden. In diesem Fall wird im folgenden Schritt 45 die Benutzeroberfläche 81 in einen neutralen Zustand gebracht, in dem inhaltlich keine Daten 85 angezeigt werden, im folgenden Schritt 47 werden sämtliche temporären Daten gelöscht und im abschließenden Schritt 49 das Anwendungs-Programm 71,73 beendet. Nach Beendigung des Anwendungs-Programms 71,73 läuft lediglich das Betriebssystem 79 in Schritt 3, wobei die Zugriffsrechte aufgrund des Anfangs in Schritt 1 erfolgten log-in's am Betriebssystem so eingeschränkt sind, dass keinerlei Manipulationen möglich sind.

Bei Eintreten bestimmter Bedingungen, z.B. bei Zeitablauf, kann in Schritt 51 die Bildschirmschoner-Instanz 76 aktiviert werden, die einem herkömmlichen Bildschirmschoner ähnlich arbeitet. Dies führt dazu, dass im folgenden Schritt 53 die Benutzeroberfläche 83 in einen inhaltlich neutralen Zustand gebracht wird, so dass keinerlei Daten 85 angezeigt werden. Der vorherige Zustand der Daten und der Benutzeroberfläche 81 wird jedoch zwischengespeichert, um ggf. nach Deaktivierung des Bildschirmschoner-Instanz wieder zur Verfügung zu stehen.

Aus diesem Zustand heraus kann die Bildschirmschoner-Instanz 76 nur dadurch deaktiviert werden, dass die zuvor beschriebene Anmeldungsprozedur in Schritt 7 erneut aufgenommen wird. Im Gegensatz dazu würde ein herkömmlicher Bildschirmschoner durch ein Bildschirmschoner-Passwort deaktiviert werden, das generell oder vom vorhergehenden Nutzer vorgegeben ist und evtl. nicht jedem Nutzer bekannt wäre.

Das in FIG 2 dargestellte Flussdiagramm macht deutlich, dass die Anmeldung von Benutzern und der Wechsel zwischen Nutzern ohne einen Neustart der Anwendungs-Programme 71,73 oder des Betriebssystems 79 erfolgt. Authentifizierung und Neu-Authentifizierung erfolgen stattdessen durch die Authentifizierungs-Instanz 75 bei laufendem Anwendungs-Programm 71,73 und Betriebssystem 79 und erfordern daher ein Minimum an Zeit. Gleichzeitig werden Zugriffe gemäß der Datenschutzbestimmungen kontrolliert und laufend protokolliert. Aufgrund seiner hohen Geschwindigkeit ist das Verfahren auch an zeitkritischen Arbeitsplätzen einsetzbar, so dass auch dort eine vollständige Protokollierung unter Angaben jeweils aktueller Daten zur Nutzeridentität möglich wird.

Das erfundene Verfahren kann auf einer Datenverarbeitungseinrichtung ablaufen. Es kann als Computer-Programm realisiert sein, das auf einer Datenverarbeitungseinrichtung ausgeführt werden kann, um das erfundene Verfahren darauf ablaufen zu lassen. Es kann als Programm auf einem Datenträger, z.B. einer Diskette, einem Festplattenspeicher oder einem sonstigen Speichermedium, gespeichert sein, der in Wechselwirkung mit einer Datenverarbeitungseinrichtung treten kann, um das erfundene Verfahren darauf ablaufen zu lassen.

Patentansprüche

1. Verfahren zum Anmelden eines Nutzers an einer Datenverarbeitungseinrichtung mit einem Betriebssystem (79) und einem Datenverarbeitungs-Programm (71, 73), wobei in einem ersten Schritt (7, 9) Daten zur Authentifizierung des Nutzers ermittelt werden, in einem zweiten Schritt (13) in Abhängigkeit von den Authentifizierungs-Daten eine Identität und ein Zugriffsrecht festgelegt werden, und in einem dritten Schritt (29) in Abhängigkeit von dem festgelegten Zugriffsrecht der Zugriff auf das Datenverarbeitungs-Programm (71, 73) und/oder auf sensible Daten (85) freigegeben wird,
d a d u r c h g e k e n n z e i c h n e t , dass die Schritte unabhängig von einem Starten des Betriebssystems (79) oder der Datenverarbeitungsanwendung (71, 73) sind.

2. Verfahren nach Anspruch 1, wobei in Abhängigkeit von der Festlegung des Zugriffsrechts eine Benutzeroberfläche (81) dargestellt wird,
d a d u r c h g e k e n n z e i c h n e t , dass durch einen Nutzerwechsel-Verfahrensschritt (37) erneut mit dem ersten Schritt (7, 9) begonnen wird, und dass die Benutzeroberfläche (81) bis zur erneuten Festlegung eines Zugriffsrechts (13) inhaltlich unverändert bleibt.

3. Verfahren nach Anspruch 2,
d a d u r c h g e k e n n z e i c h n e t , dass die Benutzeroberfläche (81) in Abhängigkeit von der erneuten Festlegung eines Zugriffrechts (13), das einen geringeren Umfang als das zuletzt festgelegte Zugriffrecht aufweist, inhaltlich reduziert wird (17, 19).

4. Verfahren nach Anspruch 3,
d a d u r c h g e k e n n z e i c h n e t , dass ein Warn-Hinweis auf die bevorstehende inhaltliche Reduzierung (17, 19) der Benutzeroberfläche (81) ausgegeben wird, und dass ein Nutzer Gelegenheit erhält, das Verfahren vor der Re-

duzierung (17, 19) erneut mit dem ersten Schritt (7, 9) beginnen zu lassen.

5. Verfahren nach Anspruch 1 bei dem in Abhängigkeit von der Festlegung eines Zugriffsrechts eine Benutzeroberfläche (81) dargestellt wird,
d a d u r c h g e k e n n z e i c h n e t , dass durch einen Nutzerabmeldungs-Verfahrensschritt (39) die Benutzeroberfläche (81) inhaltlich gelöscht wird (41) und erneut mit dem ersten Schritt (7, 9) begonnen wird.

6. Verfahren nach einem der vorhergehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t , dass sämtliche Zugriffe auf das Datenverarbeitungs-Programm (71, 73) und sämtliche Zugriffe auf sensible Daten (85) unter Angabe der jeweils festgelegten Identität protokolliert werden (33).

7. Verfahren nach einem der vorhergehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t , dass durch einen Bildschirmschoner-Schritt (51) bei Eintreten vorgegebener Bedingungen, z.B. Zeitablauf, die Benutzeroberfläche (81) für einen Nutzer unkenntlich gemacht wird (53) und erneut mir dem ersten Schritt (7, 9) begonnen wird.

8. Verfahren nach einem der vorhergehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t , dass in Abhängigkeit von einem fehlgeschlagenen Versuch der Authentifizierung eines Nutzers im ersten Schritt (7, 9) sämtliche Zugriffsrechte gesperrt werden (11).

9. Computer-Programm
d a d u r c h g e k e n n z e i c h n e t , dass es auf einer Datenverarbeitungseinrichtung ausführbar ist, um ein Verfahren gemäß einem der Ansprüche 1 bis 8 ablaufen zu lassen.

10. Datenträger

d a d u r c h g e k e n n z e i c h n e t , dass darauf ein Programm gespeichert ist, das in Wechselwirkung mit einer Datenverarbeitungseinrichtung treten kann, um ein Verfahren gemäß einem der Ansprüche 1 bis 8 ablaufen zu lassen.

Zusammenfassung

Verfahren zum Anmelden von Nutzern an Datenverarbeitungseinrichtungen

Die Erfindung betrifft ein Verfahren zum Anmelden eines Nutzers an einer Datenverarbeitungseinrichtung mit einem Betriebssystem (79) und einem Datenverarbeitungs-Programm (71, 73). In einem ersten Schritt (7, 9) werden Daten zur Authentifizierung des Nutzers ermittelt, in einem zweiten Schritt (13) in Abhängigkeit von den Authentifizierungs-Daten eine Identität und ein Zugriffsrecht festgelegt, und in einem dritten Schritt (29) in Abhängigkeit von dem festgelegten Zugriffsrecht der Zugriff auf das Datenverarbeitungs-Programm (71, 73) und/oder auf sensible Daten (85) freigegeben. Gemäß der Erfindung sind die Schritte unabhängig von einem Starten des Betriebssystems (79) oder der Datenverarbeitungsanwendung (71, 73). In einer besonders vorteilhaften Ausgestaltung der Erfindung kann ein Nutzerwechsel durch Abmelden des Nutzers und Anmelden eines neuen Nutzers stattfinden, bei dem der Anwendungs-Kontext, also Benutzeroberfläche (81) und aktuell bearbeitete Daten (85) erhalten bleibt.

FIG 1

FIG 1

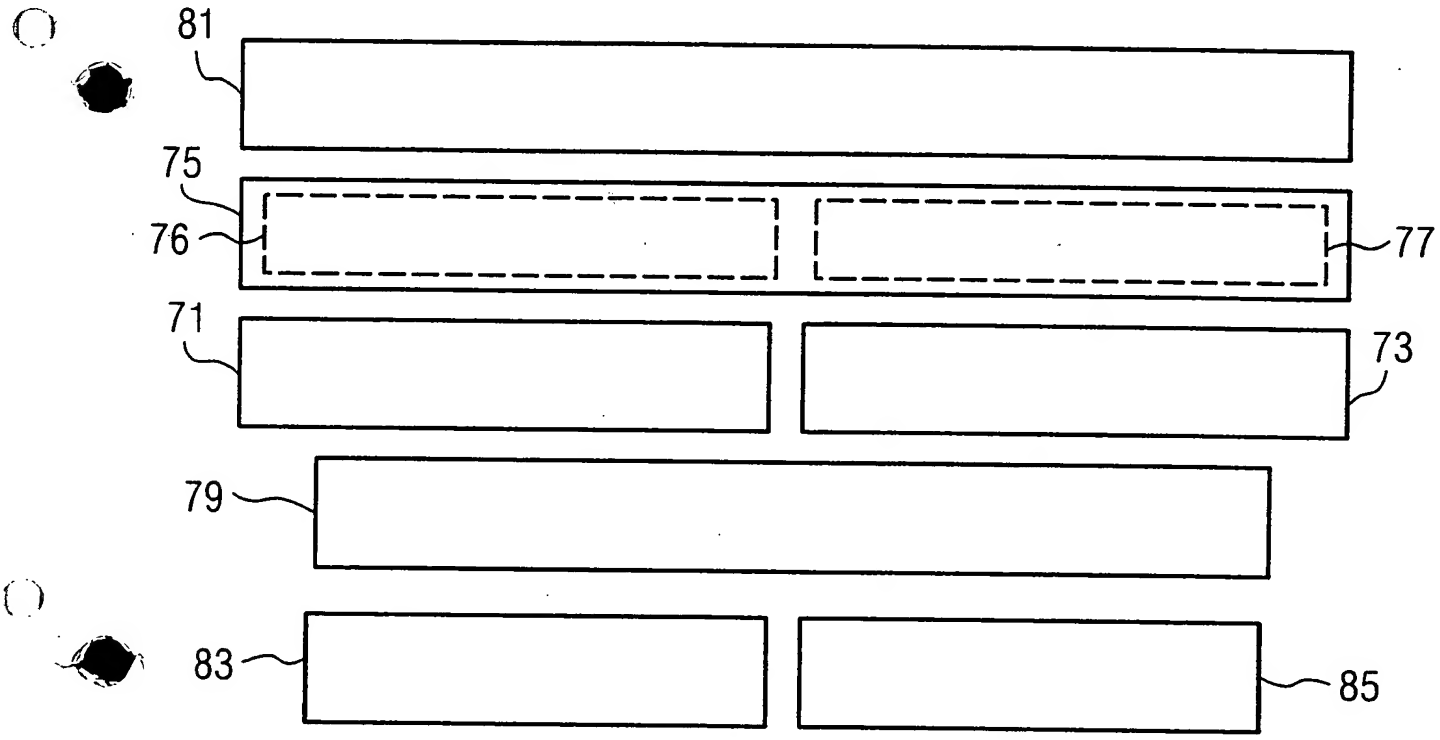

FIG 2